Release Notes for RFS6000 v3.2.0.0-040R

Contents

1. Introduction
2. Supported Hardware
3. Download Information
4. RF Firmware Versions
5. Installation Guidelines
   5.1. Upgrade Procedure
   5.2. Auto Install Procedure
6. Important Notes
7. Known Issues

1 Introduction

Motorola introduced in May 2008, the RFS6000, the latest addition to a family of high-performance multi-core processor-based wireless LAN (WLAN) switches, targeted at mid-sized enterprises. The RFS6000 supports an all-wireless enterprise vision, enabling businesses to build an enterprise WLAN that serves the entire organization from workers in corporate headquarters to manufacturing and distribution plants to remote branch offices.

WiNG v1.2 which maps to RFS6000 v3.2 is the second feature release on the RFS6000 platform. WiNG v1.2 is a minor feature release for Motorola's Enterprise-class RF & Wireless Switches that enables a Wireless Enterprise by introducing locationing services, optimizing network performance for increased user mobility-experience and delivering business continuity with increased high-availability and manageability features.

Key features in WiNG v1.2 (RFS6000 v3.2) are:

- **Locationing with *Smart Opportunistic Location Engine* (*SOLE*):** WiNG 1.2 brings the SOLE infrastructure to WiNG architecture that will enable delivery of numerous locationing services (both organic as well as 3rd party). Asset tracking, resource monitoring, and visibility solutions for security or improved workflow management with WiFi or RFID tag detection has applications across many different verticals like oil, healthcare, retail distribution, and airline.

- **Increased Manageability with:**
  Automatic upgrade of AAP firmware: WiNG v1.2 introduces an optional automatic AAP firmware upgrade procedure. The switch can now automatically detect old or incompatible firmware on the AAP and push an upgrade to the Access Point**.** This leads to decreased management and operational overhead in the network for bulk image upgrades. ***Upgrades are supported for v2.1 onwards on the Adaptive AP 51X1****.*

- **Increased network performance, mobility and business continuity with:**
  MU-rate limiting: With this feature now network managers can instrument client-based granular bandwidth control. This would preempt a client or MU from hogging network bandwidth leading to increased network performance, differentiated services and increased user mobility experience.

  MU-load-balancing: v3.2 on the RFS6000 introduces intelligence in the network to load balance MU's across Access Ports depending upon the utilization of AP's in the network, based on throughput or user count. Dynamic allocation of resources would lead to efficient network resource utilization and increased network performance.

  Redundancy Enhancements: With WiNG1.2, now not only do AP's adopt to secondary WiNG switches in the network when the primary switch becomes unavailable, but also when the primary switch loses external gateway/WAN connectivity. This ensures uninterrupted end to end network connectivity with a clustered deployment of the Motorola WLAN solution.

Functional Enhancements include:

1. Ability to upgrade the WIPS sensor image through CLI
2. MU ACLs for Adaptive APs
3. HotSpot Enhancements include:
    a. 12 hour AM/PM time format
    b. User logout upon closing of web browser

2 Supported Hardware Platforms and Changes to Software Functionality

Please note that RFS6000 v3.2 software can be applied only to the RFS6000 switch.

- RFS6000 v3.2 only works with v2.1 of the Adaptive AP 51X1. V2.0 on the Adaptive AP is not compatible with v3.2 on the RFS6000.
- The Adaptive AP firmware upgrade capability can only be used to upgrade v2.1 onwards on the AP51X1.
- All other features are supported on the AP 300 802.11 a/b/g Access Port only.

3 Download Information

To download this Software Release, please go to http://support.symbol.com from the Guided Search menu enter "RFS6000" and Document Type of "Software Downloads" then click on GO to display the available software. This is entitled software. A service contract is required for software download access to any updates created . If you are a new user, please follow the directions to create an account on Support Central and then use the serial number of your RFS6000 to request the software download.

4 RF Firmware Versions

The following RF versions are supported for the following Access Ports and Access Points:

Model	Version
AP100 (CCRF-2050)	02.05-00
AP300 (WSAP-5110; WISPe)	01.00-2100r
AP4131	07.00-08
AP300 – WIPS Sensor	00.00-04 displayed in the wireless switch/ fw 4.5.0.10
AP4131 Revert Image	00.00-00

5 Installation Guidelines

For accessing the Graphical User Interface (GUI) of the RFS6000 switches, the following browsers (and Java versions) are supported:

- Internet Explorer 6.0, 7.0 on Windows 2000, XP (JRE 1.4.2)
- Mozilla 1.4.3 on RedHat Linux (tested with JRE 1.5)
- Firefox 0.8 or higher on Windows 2000, XP (JRE 1.4.2)
- Firefox 1.0 or higher on RedHat Linux (tested with JRE 1.5)

5.1.1 Detailed Firmware Upgrade Procedure

This section outlines the upgrade procedure to v3.2 applicable if the RF switch had a beta release installed.

The method described in this section uses the Command Line Interface (CLI) and GUI and the Auto-Install procedures. To log into the CLI, either SSH, Telnet or serial access can be used (whichever exists).

Upgrading from a previous v3.2 Beta or engineering build (v3.2.0.0-xxxB)

1. Copy the RFS6000_v3.2.0.0-040R.img to your tftp/ftp server.
2. Use the "**upgrade ftp://<ip address of server>/<name of file>**" command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the switch. From CLI the command is "reload".

5.2 Auto-Install Process

Auto Install in v3.2 works via the DHCP server. This requires the definition of a Motorola Vendor Class and four sub-options under option 43 namely:

- Option 186 - defines the tftp/ftp server and ftp username, password information
- Option 187 - defines the firmware path and file name
- Option 188 - defines the config path and file name
- Option 189- defines the RFS6000 ip address to where a L3 AP300 RF port or Adaptive AP 51X1 will be adopted
- Option 190 - defines the cluster config path and file name.

The individual features (config, cluster-config and image) may be enabled separately via the CLI, snmp or Applet. If a feature is disabled then it will be skipped when Auto install is triggered.

For the static case, where the URLs for the configuration and image files are not supplied by DHCP, the URLs may be specified via the CLI, snmp or Applet. The CLI may also be used to define the expected firmware image version. If the image version is not specified we will attempt to derive it from the file name, if it can not be derived from the filename then the system will simply attempt to load something other than what it is currently running.

Configuration files are tracked by their MD5 checksum, so if a file is renamed it will still have the same md5 sum. Once a file has been loaded it will not be reloaded, even if the local configuration information is changed.

The requested image file version, if any, is checked against the current version before any attempt is made to load it. If the requested version is the same as the running version then no further action is taken. If the image file version, embedded in the file header, does not match the expected version then no further action will be taken. If the version has not been specified then the header of the image file will be compared to the local version, if they are the same then no further action will be taken.

Please note that once the system has been operating for ten minutes, Auto Install is disabled, though it may still be reconfigured. This is to prevent the system from attempting to re-install each time a DHCP lease is renewed.

Configuring Auto Install via the CLI

There are three compulsory and four optional configuration parameters.

The compulsory parameters are:

- configuration upgrade enable
- cluster configuration upgrade enable
- image upgrade enable

Optional (only for the static case):

- configuration file URL
- cluster configuration file URL
- image file URL
- expected image version

The three enables default to yes, the URLs and the version default to "" (blank)

```
RFS6000(config)#show autoinstall

feature    enabled      URL

config       yes         --not-set--

cluster cfg  yes         --not-set--

image        yes         --not-set--

expected image version  --not-set--
```

The three enables and the expected version affect any mode of operation; the URLs are only used for the static (non DHCP option) mode.

Enables are set using the **autoinstall <feature>** command:

```
RFS6000>enable
RFS6000#conf t
RFS6000(config)#autoinstall image
RFS6000(config)#autoinstall config
RFS6000(config)#autoinstall cluster-config
```

After this configuration, any switch reboot with DHCP enabled on the port will trigger Auto Install, provided the DHCP Server is configured with appropriate options.

After the reboot switch would try to acquire the IP address from DHCP server. The DHCP server will provide the auto-install parameters like image, config and cluster-config files and paths provided if they were configured in DHCP server. Based on the parameters switch downloads the corresponding files from the specified server and reboots the box again in order to take effect the newly downloaded configurations. After the switch auto-reboot, the config and cluster-config (whichever) downloaded as part of auto-install will be applied to the switch becomes switch's running-config.

NOTE: The cluster-config will be applied to the running-config but not auto saved to the startup-config. If user wants to reboot the box again for any reason, must save the running-config using the command "write-memory". Otherwise on the next boot, switch will have only the startup-config and not the cluster-config in running-config.

The "enables" are cleared using the **no autoinstall <feature>**

URLs and the version string are set as text and can be cleared by using an empty pair of double quotes to denote the blank string. In the following example we define the three URLs and the expected version of the image file and then enable all three features for Auto Install

```
RFS6000(config)#autoinstall config url
ftp://ftp:ftp@192.9.200.1/RFS6000/config

RFS6000(config)#autoinstall cluster-config url
ftp://ftp:ftp@192.9.200.1/RFS6000/cluster-config

RFS6000(config)#autoinstall image url
ftp://ftp:ftp@147.11.1.11/RFS6000/images/RFS6000.img

RFS6000(config)#autoinstall image version 3.2.0.0-040R

RFS6000(config)#autoinstall config

RFS6000(config)#autoinstall cluster-config

RFS6000(config)#autoinstall image

RFS6000(config)#show autoinstall

feature    enabled      URL

config       yes        ftp://ftp:ftp@192.9.200.1/RFS6000/config

cluster cfg  yes        ftp://ftp:ftp@192.9.200.1/RFS6000/cluster-config

image        yes        ftp://ftp:ftp@147.11.1.11/RFS6000/images/RFS6000.img

expected image version  3.2.0.0-040R
```

Once again, for DHCP option based auto install the URLs will be ignored and those passed in by DHCP will not be stored.

Whenever a string is blank it is shown as **--not-set--**.

6 Important Note: RFS6000 Port Configuration

1. ***RFS6000 v3.2 only works with v2.1 of the Adaptive AP 51X1. V2.0 on the Adaptive AP is not compatible with v3.2 on the RFS6000.***
2.
3. It may seem that the RFS6000 retains the old default gateway and ignores the latest default gateway IP address. The explanation is that: Default gateway is the 0/0 route.
   For any route that is added to nsm(network services module), when there are multiple routes to the same destination, nsm will pick ONE of them and select it to become the ACTIVE route. The active route is shown by the "show ip route" command. All routes (both active and inactive) can be seen using the show "show ip route detail command". The route with the '*' next to it is the active route.

   Only the Active route is deposited in the kernel.

   NSM uses number of ways to figure out which route should be active. e.g. Static has priority over DHCP, If nexthop is not active, the route is automatically inactive, as more routing protocols such as rip, ospf get added, distance will be used.

   When you have two static routes added both to the same destination, in this case 0/0 -> only one of them will be made ACTIVE (the first one whose next hop is active). Use "show ip route detail" to see both routes.

4. For the Adaptive AP, ***the Independent and Extended WLANs must be on unique VLANs***. Additionally, with this release, upstream WAN links of up to 2 Mbps are supported.

5. For the Adaptive AP 51X1, L3 Mobility, Rogue AP Detection and WLAN Bandwidth Management are not supported on the Wireless Switch, when in Adaptive AP mode.
6. With the Adaptive AP, the number of VLANs/WLANS supported is 15.
7. Please be aware that on a hotspot authentication success page, pressing backspace on the screen restarts the time elapsed counter. However, session timeout at the back end will still remain the same.
8. In case of login issues to the applet, it is recommended to clear the java cache for the browser
9. For Security Schemes using a passphrase, user should not use "\" for in the string.
10. ***When manually adding radios for Adaptive APs on the wireless switch, please specify AP5131 where appropriate. The AP 300 is the default value.***

7 Issues Fixed in this Release

SPR	Description
13351	After changing admin password to include a dollar sign, a login failed error is received in the GUI.
13357	When multiple VLANs are defined in either port, only the Native VLANs can be reached
13402	An IP address with a leading zero, e.g. 192.168.010.112, the IP will not be entered correctly.
13416	IPSec tunnel / HotSpot functionality / ACL list
13453	AP300s rebooting under WiNG.
13477	MC9090 and Switch - Radio power output issues.
13508	MUs Sporadically Fail WPA Authentication
13548	MU1 cannot communicate with MU2, if MU roams to an AP from switch 1 to another AP in switch 2(in a cluster)
13550	ebtables causing L3 connectivity issue with switches
13597	BC/MC to APs with no MUs associated
13631	Zebra printers periodically loose connectivity when an MU connected to the same AP goes into PSP
13633	snmpd crashes when it tries to close a session to an unresponsive agentx subagent.
13664	WPA2/CCMP security does not except 63 ASCII Characters, which is supported.
13700	fix-windows-dhcp enable parameter is lost after a reboot / reload of the switch
13707	Multicast Mask not being supported with encryption types that don't involve reply counters, like WPA.
13812	https redirect in Hotspot WLAN doesn't work
13958	802.11a radio regulation issues with Country code Japan
13964	Connectivity issues with windows terminal server cluster.
14018	In WPA - MU should be allowed to transmit and receive direct data after 4-way handshake
14064	ccsrvr crashes when walking MuProbeStatusTable
14069	AP300 11a locks up when 11bg is set to detector mode
14086	Maximum of 10 rules displayed in applet for mac extended acl list
14124	AP300 displaying incorrect VLAN on GUI and CLI, though AP300 is connected to correct VLAN
14177	The ldap configuration is lost after switch reboots if the ldap configuration has a space included.
14178	Switch doesn't reset power save state of the MU upon association
14180	GUI resets to factory default when AP4131 is adopted with a high index value.
14193	"show wireless sensor" doesn't display any APs after first missing one
14238	Wireless: AP got readopted while doing continuous roaming and authenticating with radius server
14326	% Error: invalid radio description % Invalid input detected at '^' marker. Errors received from reproduction steps
14331	Cluster-cli not working properly
14343	WM-MC9090 WM5; PEAP/MS CHAP v2 with installed self-signed Trustpoint server cetificate fails to allow client auth.
14348	Diag crash when sending SNMP trap for TRAP_FREE_RAM_LOW
14362	EAP-TLS radiusd process 100% CPU utilization

14369	Nortel branded spectra-link phones experience resets frequently.
14398	Need to support UTF-8 encoding for LDAv3 Radius
14432	sh wi mo association-history command reports an unformatted timestamp
14433	DDNS is not working properly on a /22 network
14433	DDNS :PTR records are not getting updated for /22 network while using onboard DHCP server
14448	When executing the command `show run' from the cluster-cli. the user is kicked out of cli
14504	AP is not adopting to the preferred switch
14551	Passwords that contain special characters work for a CLI login but not a GUI login
14558	AP100 radio shows up as AP4131 in GUI
14625	CLI allowing “all-11g” to be input.
14632	Not able to set the DTIM values in the Access Port Adoption Defaults if there is no AP adopted to the Switch:
14656	Importing a server certificate in PEM format to the switch fails.
14656	Core file is generated in the switch after importing the server certificate in 3.0.4.0-001B
14669	Cannot Authenticate Users To External LDAP - Novell E-Directory
14698	LDAP allows administrator to select all EAP and Auth Type and/or MSCHAPV2 types.
14798	Not sending WNMP roam notifications on behalf of MUs
14818	Random AP300 reset
14835	snmp traps cause snmpd and other services to hang and get restarted
14840	GMT+/- timezone are calculated backwards
14845	ccsrvr crash on IDS_EXCESSIVE_AUTH_FAILS
14865	radius configuration parameters lost during install of startup config file
14900	CPULoad is high but wrong % is printed
14946	Radius Hotspot/Groups/Guest Groups and User configuration/authentication issue
15047	AAP: RSS on Single Radio AP-5131 is not working for Independent WLANS
15063	Hotspot - even if user is deleted - he can still login unless he will logout
15074	AP5131 doesn't respond to pings. Appears to be wireless interference that keeps it from responding.
15077	Cannot export default_shh_rsa_key file using local disk option.
15180	when removing Telnet from USER access mode SSH does not operate.
15183	AP-Switch Tunnel setting for Adaptive AP does not set properly when imported.
15185	Access Port Status shows incorrect serial numbers for the AP5181 and AP5131.
15186	Help button on the Multiple Spanning Tree page of the GUI does not work
15215	When you deactivate a WLAN on the wireless switch, it remains active on the AAP (single radio).
15225	VLAN configuration is not persistent across reboots.
15244	Configuring Domain Name via GUI does not display in running and/or startup-config.
15259	CLI help indicates AP300 will be converted to Wireless IDS not Wireless IPS sensor.
15332	Unable to revert the AP5131 from the redundant switch.
15335	Nortel phone experience issues - AP300 locks up with b/g rates
15342	Hotspot Radius Re-authentication fails for force user to re-authenticate.
15379	CCSRV crash - bad radio index
15383	Internal RADIUS server issue with AAP
15386	AP100 adopted but no MUs can associate.
15398	Multiple ipsec SA's seen.
15450	Autoinstd service does not validate data before running.
15457	Creating user with Network Administrator role does not allow you to configure wlans/vlans
CQ 45208	Adaptive AP: Proxy-radius with Adaptive-AP will not work if a supplicant does not send realm information.

7 Known Issues

CRID/SPR	DESCRIPTION	Resolution/Workaround
SPR 14885/ CQ 46477	Intermittent/random drop offs of the switches and complete lockups at several locations	Verify that there are no speed/duplex mis-matches between the RFS7000 and the attached device. A valid work around is to not use 100mb Half-Duplex, if this issue is observed.
32426	IPSEC: Remote VPN clients connected to the switch will not be able to communicate with each other.	This will only affect remote VOIP clients communicating with each other.
SPR 15064	Hotspot - same credentials can be used to login from several laptops	Next release
SPR 15260	CA50 voice problems on WS5100	Next release
SPR 15573	Wireless Filter CLI accepts range of 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF	Next release
SPR 15576	WMM-Power Save problem on AP300	Next release
SPR 15587	426 Error received when pulling config from Windows 2000 IIS FTP to the WS5100 switch	Next release
SPR 15609	Services Summary Screen in GUI shows DHCP is Disabled when it is actually Enabled.	Next release
SPR 15148	Not able to modify the snmpmanager/trap/user passwords and import to another switch	Next release
43735	IPSEC: “Deny” rules in Crypto ACLs will be ignored.	Currently in VPN implementation, the priority to the traffic is given as below. 1) If there are permit rule first match to that rule if the rule matches the traffic is sent on the tunnel. 2) By default if none of the permit rules matches then send the traffic in plain text (don't send over tunnel)
44229	Adaptive AP: Idle-timeout parameter cannot be configured for Mobile-devices associated to an Adaptive AP.	This functionality is available on the switch, when used with the AP300, but not supported when used with the AP51X1 as an adaptive AP.
44270	Adaptive AP: Maximum number of Mobile-devices per radio on an Adaptive-AP is 127 and is different from the limits for an AP300.	AP 51X1 supports a maximum of 127 MUs per radio.
45208	Adaptive AP: Proxy-radius with Adaptive-AP will not work if a supplicant does not send realm information.	Please specify the realm.
44103	Adaptive AP: UAPSD parameters are not displayed for Mobile-devices associated to an Adaptive-AP.	This is only a GUI issue, UAPSD is enabled on the back end
44250	VPN: Remote VPN client session cannot not be established with the switch if the client is behind a NAT device.	
41870	Rogue AP: Duplicate entries are recorded in the Approved and unapproved AP list if two detectors detect the same AP.	
42521	Kerberos : WLAN gets authenticated successfully by a KDC Server even when "Use DES Encryption type" is not enabled	
45167	Adaptive AP: Hotspot configuration for Independent WLANs on an Adaptive-AP cannot be configured from the switch.	The configuration does get pushed for the extended WLAN and therefore allows for a centrally configurable and manageable hotspot

CRID/SPR	DESCRIPTION	Resolution/Workaround
43606	User Account with a (') character in password causes login failure	Please refrain from using (‘) special character in the switch login password
44971	Adaptive AP: Adaptive AP cannot be adopted using the secondary IP address of a Switch Virtual Interface (VLAN interface).	Please use the primary IP address
45537	Not able to Login through the applet (times out) when the secondary radius authentication is used	
39446	Console hangs in the case of excessive static NAT entries	System is fine with up to 128 NAT entries but there is a 15 second delay
39860	Mixed mode environment with switches running Wi-NG and Non-WiNG architecture is not supported.	Please ensure all switches are on the Wi-NG architecture code base
39490	Unit of measurement for MU statistics may not be seen	Currently, only a decimal value is seen – this should be interpreted as a percentage value.
35641	MSTP loops is not backward compatible with Rapid-PVST in Cisco switch	Rapid PVST and MSTP are two different protocols. Rapid PVST is a Cisco proprietary protocol, not an IEEE standard, and so not supported by RFS7000 When connecting RFS7000 to a Cisco please configure the Cisco switch to operate in MSTP mode
38663	TTLS/PEAP MSCHAPv2 combination doesn't work with onboard radius server using windows active directory as data source.	To be resolved in a later release
37592	The discovered switches are lost after a reboot	Work around: If you just reload the switch and keep the browser open the dropdown box with the other switches IP will remain.
39552	IP address in with leading zeros aaa.bbb.ccc.ddd format to a target server (to transfer a file or firmware) is not working i.e. 192.168.2.1 works but not 192.168.002.001	To be resolved in a future release
40110	Radius server restart to pick up configurations changes takes 2 minutes if 5000 radius users are present.	The config change will be picked up, but it takes 2 minutes for radius service to start itself once it had stopped to pick up the config changes. During this period any eap authentication or hotspot authentication tried will get failed.
39653	Switch console may hang for 20 minutes when large configuration file is copied to running config	When you load large configuration by copying to running-config, it may be slow. The recommended approach is to copy to startup config and reload the switch - this is much faster.
37280	Not possible to clear the DDNS IP bindings from the switch from CLI,APPLET and SNMP	The work around is that the DNS server which is managed by IT can clear the database using separate commands
37094	No option to enable portfast on interface from applet	Can be applied through CLI: In CLI int ge1# spanning-tree port-fast
37113	There is no warning message when user tries to Delete an ACL which specifying interesting traffic for NAT	

CRID/SPR	DESCRIPTION	Resolution/Workaround
40183	Network > Access Port Radios > WLAN Assignment page display incorrectly and "Index" filter not functioning	This only happens when the user is frequently switching between tabs. A refresh of the screen displays the right values.
36603	GUI support to convert AP to sensor and Sensor to wispe is currently not available	Currently CLI support exists to convert an AP to sensor and to revert a sensor to WISPe AP. * convert-ap 1 sensor * sensor 1 revert-to-ap * sensor VLAN 1
36996	Changing username/password for AP port authentication doesn't take effect immediately.	A reset or power off/on is currently required.
38734	GUI (Applet), "Apply" button under the Diagnostics -> Environment -> Temperature Sensor menu does not get enabled when user begins changing values for High or Critical Limit.	If you tab out of the field the APPLY button / select another field, then APPLY button will be enabled.
50806	CCSRVR core dump deleting Radio's	When manually adding radios, to specify 5131 as AP 300 is default.
42155	Wireless-Regulatory: Outdoor channels are allowed in configuration from Applet and CLI though invalid per Regulatory v0.9	This is a display issue only.
50494	AAP: Hotspot authentication for independent WLAN, using AP5131's on-board RADIUS fails	Please use an external RADIUS or the Onboard RADIUS on the Wireless Switch.
50187	Detector APs may reboot when browsing through the Rogue AP report.	No network disruption, as this only affects detector mode APs.
48343	AAP/applet: User cannot select AP image from the GUI on AAP firmware page, for USBs.	The following USBs have been tested to work and do not have the problem: • Memorex traveldrive 2.0GB (USB 2.0) • Kingston DataTraveler 1.0BG • Memorex traveldrive 8.0GB (USB 2.0)
49475	Secondary LDAP Server doesn't failover when primary LDAP server is unreachable in the Radius authentication	The workaround for this problem is that the administrator has to delete the primary LDAP server manually.
50642	Telnet session goes to diag mode when switch login authentication is done against an external radius server.	It is only telnet session which goes into diag mode and not the switch as such, the telnet session needs to be quit and a new session can be established which succeeds. No need to power cycle or reset the switch.
48882	AAP FW Upgrade failed when upgrade file is on cf and ftp root dir is also cf	The upgrade image has to be named as "aap_fw_image" and be present in the root of cf or usb and the same external drive has to be configured as the ftp root to get this working.

CRID/SPR	DESCRIPTION	Resolution/Workaround
48915	IPSEC - ISAKMP Aggressive mode settings doesn't works	This can be configured as follows to work: On SW1(IP 10.10.10.45) ======-============ crypto isakmp key 0 test12345 address 10.10.10.250 crypto map map2030 10 ipsec-isakmp set peer 10.10.10.250 match address aclstos set mode aggressive set transform-set tfset On SW2 (IP10.10.10.250) ==================== crypto isakmp key 0 test12345 address 10.10.10.45 crypto map map2030 10 ipsec-isakmp set peer 10.10.10.45 match address aclstos set transform-set tfset set mode aggressive
48827	USB: Drive mapping changes when an USB Flash drive is unplugged and plugged back while data transfer is in progress	Please do not unplug the USB while it is in process.
46137	The conversion process begins by resetting AP and provides a FAT ap image when AP is requesting runtime image. The there are multiple switch in the cluster, when switch A initiating the conversion process, AP is often adopted by switch B interrupting the conversion process.	With the clusterswitch running WiNG v1.1 or older, one needs to configure the switch to deny the AP by 1). Deleting the radio configurations for both radio 2). no adopt-unconfig-radio enable With WiNG v1.2, the workaround is to add a deny-rule to the AP's adoption-policy, without the need to delete the existing configuration. In wireless context: ap <ap-mac-address> adoption-policy deny
48426	RFID: RFID Readers do not re-adopt when a switch failover occurs in a cluster configuration	This is a feature limitation. Rnsd (RFID feature) doesn't support clustering.
50785	AP100 - Configuration of AP100 as Detector AP doesn't works from applet	Please use CLI
50469	Hotspot+Guest user+Applet: Not able to create Guest user when switch time is 00:00 (24hr format) from Applet	Guest user will not be created and it will display error as "switch date should be greater than current switch date".
50635	RTLS+AAP: Configuration of AAP coordinates under rtls does not throw any error	We do not support RTLS with Adaptive AP.
50736	assert.aplog dump seen when upgraded from 3.1.0.0-045R - radio.c,line:735,ver:01.00-2003r	When upgrading from 3.1.0.0-045R to the released version of 3.2, sometimes the AP image on 3.1 will assert and as such, an " * " will appear in the Command Line on 3.2 once it's upgraded. This condition is rare, and customers are advised to reboot the system.
49342	AAP: Deleted AAP radio will not be adopt after enabling adopt unconfigured radio.	This can be recovered by doing the following: • Delete the AAP. • Reboot the AAP. • Reboot the switch.

CRID/SPR	DESCRIPTION	Resolution/Workaround
49356	RTLS: 'reader 1 antenna 1 power' doesn't really apply to the third party reader	Please set power levels directly on the reader.
49340	SOLE: AP300 radio fails to recognize probes from the Aeroscout tags when it is set to detector mode	This is currently not supported. When an AP is designated as a detector, it does not support WLAN/BSS-mode and therefore does not forward Aeroscout packets as well.